实务公告21002：信息安全性 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/87/2021_2022__E5_AE_9E_E5_8A_A1_E5_85_AC_E5_c53_87001.htm 解释《内部审计专业实务标准)中的第 2100 条标准 相关标准：第 2100 条标准 工作性质 内部审计部门评价并帮助改进机构的风险管理、控制和治理体系。 本实务公告性质 在评价与信息安全性有关的机构治理活动时，内部审计师应该考虑以下建议。本实务指 导无意囊括开展与信息安全性有关的综合性保证活动或咨询业务必须考虑的所有方面，只是 推荐一些 高层次的审计师职责，以补充董事会和管理层的相关责任。是否遵守本实务公告 由审计师自行选择决定。 1．内部审计师应该确定管理人员、董事会、审计委员会或其他管理机构是否明确理解 信息安全性是一种管理责任。这种责任包括机构的所有关键信息，信息通过何种媒介储存则 无关紧要。 2．审计执行主管应该确定，内部审计活动拥有或有办法获取相关的审计资源，对信息 安全性和有关风险进行评价，包括内部和外部风险，以及与机构的对外关系有关的风险。 3．内部审计师应该确定管理人员是否已经向董事会、审计委员会或其他管理机构保证，一旦出现威胁机构的侵害信息安全的情况，管理人员将马上把这些情况告知内部审计人员。 4．内部审计师应该评价针对过去侵害行为和可能发生的未来侵害企图或事件的预防性、发现性和减缓性措施的有效性。内部审计师应该核证董事会、审计委员会或其他治理机构已 经通过 恰当途径获知侵害行为造成的威胁、侵害事件的具体情况、受到攻击的薄弱环节以 及纠正性措施。 5．内部审计师应该定期评价机构的

信息安全实务，在合适的条件下，加强或实施新的 控制和保卫措施，并根据评价结果为董事会、审计委员会或其他治理机构提供保证报告。这 种评价工 作既可以以独立业务的形式开展，也可以包括在其他审计或业务中以审批后的审 计计划的组成部分的形式开展。 